Notice of Allowability	Application No.	Applicant(s)	
	09/733,912	SEKI ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the RCE filed 4/15/2005*.

2. ☒ The allowed claim(s) is/are *1,3,4 and 7-11*.

3. ☒ The drawings filed on *12 December 2000* are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *5/10/2005*.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Application/Control Number: 09/733,912
Art Unit: 2131

This action is in response to the communication filed on 4/15/2005.

1. The application has been amended as follows:

EXAMINER'S AMENDMENT

2. Due to three minor errors to the status identifiers of claims 1, 3 and 11, an interview was conducted over the telephone with Sam Huang, in which authorization for this examiner's amendment was given on 5/10/2005.

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Please enter the following amendment to the claims contained on pages 3-5:

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An encryption control apparatus, comprising:

a CPU for running a program;

a ROM for storing the program run by the CPU;

a RAM used as a work area while the CPU is running the program;

an I/O section for sending/receiving data to/from an external device; and

an encryption section for decrypting encrypted data and encrypting plain text data,

wherein each of the foregoing components is formed on a single semiconductor device,

wherein the RAM stores a private key and a public key used in decrypting the encrypted data,

the ROM stores data specifying a party having an authorization to use the encryption control apparatus, and

wherein the encryption control apparatus has a standby mode for waiting for data to be received from an external device and an enable mode for enabling an operation, and further comprises mode switching means for decrypting encrypted data sent from the external device in the standby mode with the private key stored in the RAM so that the plain text data is restored, the switching means also checking whether the plain text data coincides with the data stored in the ROM, and switching the encryption control apparatus to the enable mode or back to the standby mode depending on coincidence and discrepancy of the data,

wherein the encryption control apparatus further comprises a key generating means for generating the private key and the public key, and

wherein the encryption control apparatus delivers the public key alone to the external device, and

wherein the external device receives the public key from the encryption control apparatus to encrypt the data sent to the encryption control apparatus.

2. (Canceled)

3. (Previously presented) The encryption control apparatus according to claim 2, wherein:

the ROM stores a plurality of main programs run in the enable mode; and

the encryption control apparatus further comprises main program selecting means for selecting one of the plurality of main programs run in the enable mode based on the data sent from the external device in the standby mode.

4. (Original) The encryption control apparatus according to claim 1, further comprising an authentication section, formed on the single semiconductor device, for sending/receiving data to/from an external information processing device that carries out information processing based on data sent/received to/from the encryption control apparatus, the authentication section also authenticating a data sender party to judge whether the data sender party is an authorized party.

5. (Canceled)

6. (Canceled)

7. (Original) The encryption control apparatus according to claim 4, wherein:

the RAM stores a private key used in decrypting the encrypted data;

the ROM stores data for specifying a party having an authorization to use the encryption control apparatus; and

the encryption control apparatus further comprises I/O section control means for decrypting the encrypted data received in the authentication section with the private key stored in the RAM so that plain text data is restored, the I/O section control means also checking whether the plain text data coincides with the data stored in the ROM, and enabling the I/O section only when coincidence of the data is confirmed.

8. (Original) The encryption control apparatus according to claim 7, wherein:

the single semiconductor device includes a plurality of the I/O sections mounted thereon; and

the I/O section control means enables an I/O section corresponding to the data received by the authentication section based on the authentication data.

9. (Original) The encryption control apparatus according to claim 7, wherein:

the I/O section is allowed to be set to an arbitrary security level among a plurality of security levels; and

the I/O section control means sets the I/O section to a security level corresponding to the data received in the authentication section based on the data.

10. (Original) The encryption control apparatus according to claim 4, wherein the authentication section sends/receives the data to/from the external information processing device through a modem.

11. (Previously presented) The encryption control apparatus according to claim 1, further comprising data destroying means, which upon receipt of abnormality detection, destroys a key stored in the RAM.

Response to Arguments

4. Applicant traverses primarily that:

   i. Abraham failed to disclose "a key generating means...sent to the encryption control apparatus."

   ii. Ganesan failed to disclose all the limitations of claim 1.

5. Applicant's argument i, filed 4/15/2005, with respect to claims 1, 3-4, and 7-11 has been fully considered and is persuasive.

6. Applicant's argument ii, filed 4/15/2005, with respect to claims 1, 3-4, and 7-11 has been fully considered and is persuasive. This is due to the fact that Ganesan did not teach or suggest a combination as claimed in independent claim 1, including mode switching means for decrypting encrypted data sent from the external device in the standby mode with the private key stored in RAM.

7. As such, the rejections of claims 1, 3-4, and 7-11 are withdrawn.

Allowable Subject Matter

8. Claims 1, 3-4, 7-11 are allowed.

9. The following is an examiner's statement of reasons for allowance:

10. Dillaway et al. (US Patent Number 5,742,756) disclosed a smartcard that generates asymmetric key pairs and performs other cryptographic operations and further includes mode switching means. However, Dillaway does not teach or suggest a combination as claimed in independent claim 1, including the mode switching means decrypting encrypted data sent from

the external device in the standby mode with the private key stored in RAM. As can be seen from Dillaway Col. 5 Paragraph 5 – Col. 6 Paragraph 2, the mode switching means does not decrypt the user presence code, as it is sent in plain form. Therefore, claim 1 is allowable over Dillaway.

11. Merriam (US Patent Number 6,643,781) disclosed a smartcard with mode switching means which issues a challenge and decrypts a response using a private key. However, Merriam does not teach or suggest a combination as disclosed in independent claim 1 including generating an asymmetric key pair, storing the key pair in RAM or using a private key from RAM to decrypt the challenge. As can be seen from Merriam Col. 5 Paragraph 6 – Col. 6 Paragraph 2, the asymmetric key pair was pre-established and not generated by the smartcard. Therefore, claim 1 is allowable over Merriam.

12. Matyas et al. (US Patent Number 5.142.578) disclosed a cryptographic unit for distributing symmetric keys using generated asymmetric keys. However, Matyas does not teach or suggest a combination as claimed in independent claim 1, including a mode switching means which decrypts encrypted data sent from the external device in the standby mode with the private key stored in RAM. Therefore, claim 1 is allowable over Matyas.

13. Because claim 1 is allowable over the prior art, claims 3-4 and 7-11 are also allowable by virtue of their dependency to claim 1.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Application/Control Number: 09/733,912
Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Junior Patent Examiner
Art Unit 2131
5/10/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100